Programmatic Safety Precepts

PSP-1*	The Program Office shall establish and maintain a system safety program (SSP) consistent with MIL-STD-882.
PSP-2*	The Program Office shall establish unifying safety precepts and processes for all programs under their cognizance to ensure: –Safety consistent with mission requirements, cost and schedule –Mishap risk is identified, assessed, mitigated, and accepted. –Each system can be safely used in a combined and joint environment –That all statutory safety regulations, laws, and requirements are met.
PSP-3*	The program office shall ensure that off-the-shelf items (e.g., COTS, GOTS, NDI), re-use items, original use items, design changes, technology refresh and technology upgrades (hardware and software) are assessed for safety, within the system.
PSP-4*	The Program Office shall ensure that safety is addressed for all life cycle phases.
PSP-5	Compliance to and deviation from the safety precepts shall be addressed during all Milestone decisions and formal design reviews to include SRR, PDR, and CDR.
PSP-6*	The Program Office shall ensure that UMS designs comply with current safety and performance criteria.

* Denotes applicability to both manned and unmanned systems

While the precepts serve only as a guide, usage of the terms “shall” and “should” reflects the level of concern of the safety community

Reference the UMS Safety Guide for additional precept clarification (found in Appendix E of the guide)

Operational Safety Precepts

OSP-1	The controlling entity(ies) of the UMS should have adequate mission information to support safe operations.
OSP-2	The UMS shall be considered unsafe until a safe state can be verified.
OSP-3	The authorized entity(ies) of the UMS shall verify the state of the UMS, to ensure a safe state prior to performing any operations or tasks.
OSP-4*	The UMS weapons should be loaded and/or energized as late as possible in the operational sequence.
OSP-5*	Only authorized, qualified and trained personnel, with the commensurate skills and expertise, using authorized procedures, shall operate or maintain the UMS.

Design Safety Precepts

DSP-1*	The UMS shall be designed to minimize the mishap risk during all life cycles phases.
DSP-2	The UMS shall be designed to only respond to fulfill valid commands from the authorized entity(ies).
DSP-3	The UMS shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.
DSP-4*	The UMS shall be designed to isolate power until as late in the operational sequence as practical from items such as: a) Weapons b) Rocket motor initiation circuits c) Bomb release racks or d) Propulsion systems.
DSP-5*	The UMS shall be designed to prevent release and/or firing of weapons into UMS structure or other weapons.
DSP-6*	The UMS shall be designed to prevent uncommanded fire and/or release of weapons or propagation and/or radiation of hazardous energy.
DSP-7*	The UMS shall be designed safely initialize in the intended state, safely change modes and states, and prevent hazardous system mode combinations or transitions.

Design Safety Precepts
(Cont'd)

DSP-8*	The UMS shall be designed to provide for an authorized entity(ies) to abort operations and return the system to a safe state, if possible.
DSP-9*	Safety critical software for the UMS design shall only include required and intended functionality.
DSP-10*	The UMS shall be designed to minimize single-point, common mode or common cause failures for high (catastrophic) and serious (critical) risks.
DSP-11*	The UMS shall be designed to minimize the use of hazardous materials.
DSP-12*	The UMS shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the UMS equipment.
DSP-13*	The UMS shall be designed to identify to the authorized entity(s) the weapon being released or fired.
DSP-14*	In the event of unexpected loss of command link, the UMS shall transition to a pre-determined and expected state and mode.

Design Safety Precepts
(Cont'd)

DSP-15*	The firing of weapon systems shall require a minimum of two independent and unique validated messages in the proper sequence from authorized entity(ies), each of which shall be generated as a consequence of separate authorized entity action. Both messages should not originate within the UMS launching platform.
DSP-16	The UMS shall be designed to provide contingencies in the event of safety critical failures or emergencies involving the UMS.
DSP-17	The UMS shall be designed to ensure safe recovery of the UMS.
DSP-18*	The UMS shall consider compatibility with the test range environment to provide safety during test and evaluation.
DSP-19*	The UMS shall be designed to safely operate within combined and joint operational environment.